Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм	Информациони системи и технологије
Назив предмета	01.M20013 Анализа сајбер инцидената и одговор
Наставник (ци)	Миловановић М. Милош, Ванредни професор Јовановић Д. Бојан, Доцент
Статус предмета	ИМ
Број ЕСПБ	6
Услов	Нема.
Предмети предуслови	Нема

Циљ предмета

Оспособљавање студената да разумеју контекст и појам сајберсигурности, као и њен значај сада и за будући развој информационих технологија. Упознавање са практичним алатима за анализу инцидената и могућим одговорима на њих.

Исход предмета

Студенти ће бити оспособљени да анализирају сајбер инциденте, користећи актуелне препоруке и практичне алате.

Садржај предмета

Садржај предмета
Теоријска настава
П-01 Увод у анализу сајбер инцидената и одговор
П-02 Процеси управљања ризиком
П-03 Сигурносни ризици апликације
П-04 Основе закона, прописа, политика и етике које се односе на кибернетичку сигурност и приватност
П-05 Начела кибернетичке сигурности и приватности, сајбер претње и рањивости
П-06 Основе концепата и протокола рачунарског умрежавања и методологије заштите мреже
П-07 Концепт архитектуре мрежне сигурности, укључујући топологију, протоколе, компоненте и принципе
П-08 Категорије инцидената, одговори на инцидент и временски рокови одговора
П-09 Методологије и технике детекције провале за откривање упада и мрежних упада
П-10 Методе анализе мрежног саобраћаја, анализа нивоа пакета
П-11 Различите класе напада
П-12 Основе концепата и методологија анализе злонамерног софтвера
П-13 Анализа понашања сајбер нападача
П-14, П15 Редослед и фазе сајбер напада
Практична настава
В-01, В-02 Надгледање сигурности мреже
В-03, В-04 Испитивање напада у IP мрежама
В-05 Концепти: снимање мрежних пакета
В-06 Рад са алатима Wireshark, tcpdump, netstat, nmap
В-07 Мрежни алати за анализу
В-08 MS Windows догађаји, firewall, log фајлови, процеси и регистри
В-09, В-10 Актуелни напади и одбрамбене алатке и технике
В-11 Статичка анализа злонамерног софтвера
В-12 Динамичка анализа злонамерног софтвера
В-13 Анализа злонамерних MS Windows програма
В-14, В-15 Анализа злонамерних Linux програма

Литература

Р.бр.	Аутор-и	Наслов	Издавач	Година
1,	Eric C. Thompson	Cybersecurity Incident Response	Apress	2018
2,	J.T. Luttgens, M. Pepe, K. Mandia	Incident Response and Computer Forensics	Mc GrawHill	2014
3,	Richard Bejtlich	The Practice of Network Security Monitoring USA		2013

Број часова активне наставе	Теоријска настава	Практична настава			Остали часови
		Вежбе	ДОН	СИР	
	2	2	0	0	0

Стандард 05. - Курикулум

Методе извођења наставе

Предавања, вежбе, практичан рад, консултације, студијски истраживачки рад, студије случајева
Предавања се изводе по моделу екс катедра, наставник користи обавезно припремљену презентацију коју путем пројектора приказује у учионици. Наставник по потреби користи таблу и маркер за поједине наставне јединице. Вежбе се изводе у обичној учионици, при чему наставник путем пројектора приказује припремљене презентације као и конкретне алате. Наставник користи таблу и маркер за поједине задатке. Наставник инструира студенте да подесе потребне алате на сопственим рачунарима и по моделу мешовитог приступа учењу студенти раде на сопственим рачунарима у учионици и код куће. Практичан рад се одвија по моделу дефинисања пројектног задатка, формирања пројектних тимова и потом њихове израде од стране студената, кроз редовне консултације.

Оцене знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Активност у току наставе	Да	10.00	Писмени испит	Да	40.00
Пројектни/семинарски рад	Да	50.00			